資料來源：旺報台商周報法律專欄B5版(2017/7/16出版)

網絡安全法上路 企業不容忽視

文／徐雪舫、李小明

近年隨著網絡的普及以及互聯網經濟的飛速發展，大陸地區網友的數量接近8億，網絡已深入個人生活和企業經營的各個領域當中。網絡的普及除了帶來積極的影響外，也伴隨著越來越多的網絡詐騙、非法網絡入侵以及個人信息的洩露等問題。在這樣背景下，《中華人民共和國網絡安全法》（以下簡稱《網絡安全法》）於2016年11月7日通過，並於2017年6月1日在大陸正式實施。《網絡安全法》作為大陸第一部全面規範網絡安全管理方面的基礎性法律，自制定之日起便廣受各個領域、特別是涉及經營互聯網相關業務的企業的高度關注。本文從企業的角度出發，歸納整理《網絡安全法》的重要內容並說明可能對企業帶來的影響。

《網絡安全法》規定在中華人民共和國境內建設、營運、維護和使用網絡，及網絡安全的監督管理，應適用該法。

明訂網安適用範圍

依《網絡安全法》，「網絡營運者」指網絡的所有者、管理者和網絡服務提供者。其中「網絡服務提供者」指通過網絡提供服務的相關主體。而《網絡安全法》並未對「服務」進一步限定範圍，因此該法所指的「服務」包含的範圍是非常廣泛的，不僅包括以網絡為媒介進行經營並獲取利潤的企業，如各種電商購物平台、APP應用及在線培訓平台，還包括通過網絡展開宣傳推廣等業務的各類實體企業。

界定關鍵信息基礎設施

又值得注意的是，《網絡安全法》引進了關鍵信息基礎設施的概念。《網絡安全法》規定，國家對公共通信和信息服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域，以及其他一旦遭到破壞、喪失功能或者數據洩露，可能嚴重危害國家安全、國計民生、公共利益「關鍵信息基礎設施」，在網絡安全等級保護制度的基礎上，實行重點保護，關鍵信息基礎設施的具體範圍和安全保護辦法由國務院另行制定。目前大陸有關部門正在按照《網絡安全法》的要求，加緊制定相關配套規定，其中關鍵信息基礎設施保護辦法有望近期公開徵求意見。鑑於大陸將對關鍵信息基礎設施實行重點保護，因此未來企業若被納入關鍵信息基礎設施營運者的範圍中，企業必將面臨更多的網絡安全保護義務。

雖然《網絡安全法》目前並未明確關鍵信息基礎設施營運者的具體範圍，但是卻提到關鍵信息基礎設施涵蓋「公共通信和信息服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域」，建議涉及上述領域的相關企業、機構未雨綢繆，在關鍵信息基礎設施具體保護辦法正式頒布前做好法律實施的準備工作，自覺規範網絡行為。

數據跨境傳輸的限制

《網絡安全法》的另一重要規定係有關信息的跨境傳輸。該法規定關鍵信息基礎設施的營運者在中華人民共和國境內營運中收集和產生的個人信息和重要數據應當在境內存儲。因業務需要，確需向境外提供的，應當按照國家網信部門會同國務院有關部門制定的辦法進行安全評估；法律、行政法規另有規定的，依照其規定。

關於上述規定，許多經營範圍涉及國際貿易的企業或跨國的大型零售企業可能會擔心此項規定是否會限制企業內部貿易或客戶數據跨境流動，進而影響到企業的正常經營。對此，大陸網信辦網絡安全協調局有關負責人做出了如下四點解讀：1）該法對關鍵信息基礎設施營運者提出的要求，而不是對所有網絡營運者的要求；2）不是所有的數據，只限於個人信息和重要數據，而重要數據是對國家而言，並不是針對企業和個人；3）對於確需出境的數據，法律作了制度上的安排，經過安全評估認為不會危害國家安全和社會公共利益的，可以出境；4）經個人信息主體同意的，個人信息可以出境。特別要說明的是，撥打國際電話、發送國際電子郵件、通過互聯網跨境購物以及其他個人主動行為，視為已經個人信息主體的同意。

根據《網絡安全法》的要求，大陸有關部門近期發布了《個人信息和重要數據出境安全評估辦法（徵求意見稿）》（以下簡稱《評估辦法》）和《信息安全技術 數據出境安全評估指南（草案）》（以下簡稱《評估指南》）。作為《網絡安全法》的配套法規，《評估辦法》制定了個人信息和重要數據出境安全評估的基本框架，從評估方式和評估內容等方面做出了相關規定。而作為國家推薦性標準的《評估指南》則是對《評估辦法》的細化和補充，明確了數據出境安全評估流程、評估要點、評估方法等內容。

值得注意的是，《評估辦法》規定不僅限於關鍵信息基礎設施營運者，而是要求所有網絡營運者向境外提供境內營運中收集和產生的個人信息和重要數據時進行安全評估。這較之前大陸網信辦有關負責人關於安全評估僅適用於關鍵信息基礎設施營運者的解讀是進一步擴大。在《評估辦法》中，關鍵信息基礎設施的營運者和其他網絡營運者的區別在於關鍵信息基礎設施的營運者應報請行業主管或監管部門組織安全評估，而其他網絡營運者可自行組織對數據出境進行安全評估。

觸法要承擔法律責任

為了保證《網絡安全法》的有效實施，對於違反《網絡安全法》的行為，《網絡安全法》用專門的一章內容明確了相關處罰規定，處罰措施包括責令改正、警告、罰款、責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照、對直接負責的主管人員和其他直接責任人員罰款、職業禁入、記入信用檔案等。除了上述行政處罰措施，違法者還應當承擔因違法行為而產生的民事責任和刑事責任。

總結

作為大陸第一部全面規範網絡安全的綜合性基礎性法律，《網絡安全法》的公布順應了網絡空間安全化、法制化的發展趨勢，在維護網絡健康發展，保護國家網絡安全，網絡隱私保護方面具有重大意義。但是考慮到網絡安全的複雜性和敏感性，《網絡安全法》仍留有許多空白及待決問題，如「網絡安全等級保護制度」和「關鍵信息基礎設施」都需進一步公布相關配套法規予以明確。對於目前在大陸地區的外資企業而言，只要存在著被納入《網絡安全法》適用範圍的可能，就應當對《網絡安全法》的內容和立意進行學習瞭解，並對後續《網絡安全法》的相關配套法規的制定進行持續關注，從而避免因不瞭解相關法規而給企業的經營帶來法律風險。

（作者徐雪舫是理律法律事務所資深顧問；李小明是上海律同衡律師事務所合夥律師。本文不代表理律法律事務所及律同衡律師事務所意見。）